Comment on "NMR Experiment Factors Numbers with Gauss Sums"

Mehring *et al.* have recently described an elegant nuclear magnetic resonance (NMR) experiment [1] implementing an algorithm to factor numbers based on the properties of Gauss sums. Similar experiments have also been described by Mahesh *et al.* [2]. In fact these algorithms do not factor numbers directly, but rather check whether a trial integer ℓ is a factor of a given integer N. Here I show that these NMR schemes cannot be used for factor checking without first implicitly determining whether or not ℓ is a factor of N.

The method is based on a property of truncated Gauss sums

$$\mathcal{A}_N^{(M)}(\ell) = \frac{1}{M+1}\sum_{m=0}^{M} \exp\left[-2\pi i\, m^2 \frac{N}{\ell}\right], \qquad (1)$$

namely that $\mathcal{A}_N^{(M)}(\ell) = 1$ if ℓ is a factor of N, and that its magnitude is small otherwise, thus allowing factors to be distinguished from nonfactors as long as the truncation parameter M is not too small. Mehring *et al.* in fact evaluate the closely related sum

$$\overline{\mathcal{C}}_N^{(M)}(\ell) = \frac{1}{M+1}\sum_{m=0}^{M} \cos\left(2\pi m^2 \frac{N}{\ell}\right) \qquad (2)$$

where I have neglected the effects of relaxation, which is included in their treatment but is not critical to this discussion. They achieve this by generating a set of spin echoes by applying a series of 180° pulses with phases ϕ_k given by

$$\phi_k = \begin{cases} (-1)^k (2k-1)\pi \frac{N}{\ell} & \text{for } k \geq 1 \\ 0 & \text{for } k = 0. \end{cases} \qquad (3)$$

They then proceed to demonstrate an experimental realization of the algorithm for $N = 157573$ and to discuss a numerical simulation of the algorithm for the 24 digit number $N = 106288583786304618809830 7$.

While this algorithm does in fact work, it cannot be used in any useful way. The success of the algorithm relies on the initial calculation of values of ϕ_k; this is equivalent to the evaluation of the ratio N/ℓ, and any calculation of ϕ_k must be performed with sufficient precision to indicate whether or not this ratio is an integer, and thus whether or not ℓ is a factor of N. Similar comments apply to the methods of Mahesh *et al.*

Mehring *et al.* then suggest that their method can perhaps be extended using Liouville space quantum computing [3] to provide an efficient factoring algorithm. It is difficult to comment on this as no details are provided, but it seems highly plausible that similar arguments would apply.

In passing I note that the method of Gauss sums works by determining whether or not the ratio N/ℓ is an integer, and this is only useful for identifying factors if ℓ can be confined to the integers. For example, it is easy to distinguish 17, which is a factor of 157573, from 18, which is not, by using their corresponding Gauss sums. However the trial number $157573/9268 \approx 17.0018343$ gives an equivalent peak in the Gauss sum although it obviously does not correspond to a factor.

For these reason methods based on Gauss sums will only be useful if is possible to avoid explicit division in the algorithm and the integral nature of ℓ is built directly into the implementation.

I thank Ian Walmsley for helpful discussions.

J. A. Jones
Centre for Quantum Computation
Clarendon Laboratory, University of Oxford
Parks Road, Oxford OX1 3PU, UK

[1] M. Mehring, K. Müller, I. Sh. Averbruch, W. Merkel and W. P. Schleich, Phys. Rev. Lett. **98,** 120502 (2007).
[2] T. S. Mahesh, N. Rajendran, X. Peng and D. Suter, quant-ph/0701205.
[3] Z. L Mádi, R. Brüschweiler and R. R. Ernst, J. Chem. Phys. **109,** 10603 (1998).